



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/708,547	03/10/2004	Blayn W. Beenau	60655.5900	2546

66170 7590 07/22/2010
Snell & Wilmer L.L.P. (AMEX)
ONE ARIZONA CENTER
400 E. VAN BUREN STREET
PHOENIX, AZ 85004-2202

EXAMINER

CHAMPAGNE, LUNA

ART UNIT	PAPER NUMBER
----------	--------------

3627

NOTIFICATION DATE	DELIVERY MODE
-------------------	---------------

07/22/2010

ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

HSOBELMAN@SWLAW.COM
DMIER@SWLAW.COM
JESLICK@SWLAW.COM

Office Action Summary	Application No. 10/708,547	Applicant(s) BEENAU ET AL.	
	Examiner LUNA CHAMPAGNE	Art Unit 3627	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 May 2010.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-17, 19 and 20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-17, 19-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Applicant's submission filed on 5/03/10 has been entered. Claims 1-17, 19, 20 are presented for examination. Claim 18 is cancelled.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

2. Claims 1-7, 9-12, 14, 19, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seidman et al. (US 6671358 A1), as supported by the provisional (60/286309), in view of Perron et al. (US 2002/0047049 A1), as supported by the provisional (60/230,914), in further view of Atalla (4,268,715)

3. Re claim 1, Seidman et al. disclose a system for securing a radio frequency (RF) transaction, the system comprising: a radio frequency identification (RFID) transaction device operable to send an RF transmission (See e.g. col. 2, lines 36-42).

Seidman et al. do not explicitly disclose a system comprising the transaction device including a database for storing a transaction device identifier and a transaction device authentication tag, wherein the transaction device identifier is different from the transaction device authentication tag; a transaction device random number generator for generating a transaction device random number ; a transaction device random number generator for generating a transaction device random number, the transaction device random number generator being located at the transaction device; a transmitter operable to transmit the transaction device identifier, the

Art Unit: 3627

transaction device authentication tag, and the transaction device random number; wherein the transaction device is operable for transmitting, to a RFID reader, both the transaction device identifier and the transaction device authentication tag for validation, wherein the validation is based at least in part on both the transaction device identifier and the transaction device authentication tag; and wherein the transaction device random number is used to lookup a previously stored decryption key for decrypting at least one of the transaction device identifier and the transaction device authentication tag, the transaction device random number having been received from the RFID transaction device.

However, Perron et al. disclose

-a system comprising the transaction device including a database for storing a transaction device identifier and a transaction device authentication tag, wherein the transaction device identifier (card number) is different from the transaction device authentication tag (PINs) (see e.g. paragraphs 0025, 0032 – the personalization data are stored in a non-volatile data memory 32, more particularly an EEPROM).

-a transaction device random number generator for generating a transaction device random number, the transaction device random number generator being located at the transaction device (see e.g. paragraphs 0009, 0029 – The device randomly generates an internal number using one of more different methods. This random internal number, or at least a portion thereof, can be either divided to form the serial number and the key number; the card 2 can even be designed to generate two or more random internal numbers);

a transmitter operable to transmit the transaction device identifier (identification data appearing on the card 2 itself or pre-programmed in one of its memories but used solely to verify the identity of the card 2; for example a card number embossed or otherwise written on one of the surfaces 14, 16 of the card 2), the transaction device authentication tag (Personal identification

Art Unit: 3627

numbers (PINs)), and the transaction device random number (the random internal number generated by the device) (See e.g. paragraphs 0032, 0009) wherein the transaction device is operable for transmitting, to a RFID reader, both the transaction device identifier and the transaction device authentication tag for validation, wherein the validation is based at least in part on both the transaction device identifier and the transaction device authentication tag (See e.g. paragraphs 0033 – 0034 – the serial number (from the generated random number) or any other identification number and the updated counter valued are obtained from the corresponding memory of card 2, such as the RAM 31 or the EEPROM 32, to form portions of a data stream that is to be transferred to the transaction system. Once the data stream is received, the transaction system generally finds the record of the card 2 or that of end user with the serial number or any other number and then determines with the signature if the transaction is legitimate or not).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to modify Seidman et al., and include the steps cited above as taught by Perron et al., in order to further secure transactions and determine if the transaction is legitimate (see e.g. paragraph 0034).

Seidman et al., disclose an RFID transaction device. Perron et al., disclose looking up/retrieving the records of card 2 based on the serial number/random number. Seidman et al., in view of Perron, do not explicitly disclose the steps wherein the transaction device random number is used to lookup a previously stored decryption key for decrypting at least one of the transaction device identifier and the transaction device authentication tag, the transaction device random number having been received from the RFID transaction device.

However, Atalla discloses the steps and wherein the transaction device random number is used to lookup a previously stored decryption key for decrypting at least one of the

Art Unit: 3627

transaction device identifier and the transaction device authentication tag, the transaction device random number having been received from the transaction device (see e.g. col. 4, lines 65-67; col. 5, lines 47-54 where, during a transaction, a decryption module at the processing station decrypts an encrypted message sent by a user device using a transmitted random number).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to modify Seidman et al., in view of Johnson JR, and include the steps comprising a transaction device random number used to lookup a previously stored decryption key for decrypting at least one of the transaction device identifier and the transaction device authentication tag, the transaction device random number having been received from the transaction device, as taught by Atalla, in order to provide secure data transmission, via a multilevel encryption, during the authentication of the transaction.

4. Re claim 2, Seidman et al. disclose a system further comprising: a merchant Point of Sale (POS) device in communication with the RFID reader; wherein the RFID reader is in communication with the transaction device (See e.g. col. 2, lines 43-47); and an account authorizing agent in communication with said merchant POS (See e.g. col. 17, lines 9-12).

5. Re claims 3, 4, Seidman et al. disclose a system wherein the RFID reader includes: a reader random number generator for producing a reader random number a system wherein the RFID reader further comprises: a processor in communication with the reader random number generator; and a system wherein a reader database for storing a RFID reader identifier (See e.g. col. 13, lines 17-25);

Art Unit: 3627

6. Re claim 5, Seidman et al. disclose a system wherein the transaction device random number generator is operable to provide the transaction device random number to the RFID reader, wherein the reader operable to provide the transaction device random number to the POS, wherein the POS configured to provide the transaction device random number to the account authorizing agent system (See e.g. col.13, lines 17-25).

7. Re claims 6, Seidman et al., disclose system wherein said RFID reader is operable to provide said transaction device identifier to said merchant POS (See e.g. col. 22, lines 51-59).

8. Re claims 7 and 12, it would have been a design choice, at the time of the invention, to have at least one of said transaction device identifier and said transaction device random number provided to the RFID reader in track 1/track 2 International Standards Setting Organization format, in order to synchronize the system.

9. Re claim 9, Seidman et al. do not explicitly disclose a system wherein the authorizing agent system is configured to validate the transaction device identifier in accordance with the transaction device random number (See e.g. col. 18, lines 42-51).

However, Perron et al. disclose a system wherein the authorizing agent system is configured to validate the transaction device identifier in accordance with the transaction device random number (See e.g. paragraph 0034).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention, to modify Seidman et al., and include the steps wherein the authorizing agent system is configured to validate the transaction device identifier in accordance with the

Art Unit: 3627

transaction device random number, as taught by Perron et al., in order to authenticate the device.

Re claim 10, Seidman et al. disclose a system wherein the RFID reader random number generator is operable to provide said reader random number to the POS, and wherein the POS is configured to provide at least one of the transaction device random number, transaction device identifier, and reader RFID reader random number to the account authorizing agent system (See e.g. col. 22, lines 48-59, col. 17, lines 9-12).

10. Re claims 11 and 14, Seidman et al. disclose a system wherein the RFID reader is operable to provide at least one of the transaction device random number, transaction device identifier, and reader RFID reader random number to the merchant POS; a system wherein the authorizing agent system is configured to validate at least one of said transaction device and the RFID reader, in accordance with the at least one of the transaction device random number, transaction device identifier, and reader RFID reader random number transaction device random number (See e.g. col. 17, lines 9-42).

11. Re claim 19, Seidman et al., do not explicitly disclose the system wherein the transaction device random number is converted to a validating code and then used to validate the transaction device.

However, Perron et al. disclose the system wherein the transaction device random number is converted to a validating code and then used to validate the transaction device (see e.g. paragraph 0034- Once the data stream is received the transaction system generally finds the record of the card 2 or that of end user with the serial number or any other number).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention to modify Seidman et al., and include a method wherein the transaction device random number is converted to a validating code and then used to validate the transaction device, as taught by Perron, in order to further secure transactions and determine if the transaction is legitimate (see e.g. paragraph 0034).

12. Re claim 20, Seidman et al., in view of Perron et al. do not explicitly disclose a system wherein the transaction device random number is converted to a validating code and then used to validate the transaction device; a new transaction device random number is generated for each transaction.

However, Atalla discloses a method wherein a new transaction device random number is generated for each transaction (see e.g. col. 4, lines 47-55).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention to modify Seidman et al., in view of Perron et al., and include a system wherein a new transaction device random number is generated for each transaction, as taught by Atalla, order to provide secure data transmission, via a multilevel encryption, during the authentication of the transaction.

13. Claims 8 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seidman et al. (US 6671358 A1), as supported by the provisional (60/286309), in view of Perron et al. (US 2002/0047049 A1), as supported by the provisional (60/230,914), in further view of Atalla (4,268,715), in view of further view of Official Notice.

Art Unit: 3627

14. Re claims 8 and 13, Seidman et al., in view of Perron et al., in further view of Atalla, do not explicitly disclose a system wherein at least one of said transaction device identifier and said transaction device random number is provided to said RFID reader in POS pre-defined format.

However the Examiner takes Official Notice that it is well known in the art that a recognizable format should be provided to a receiving system in a network.

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention to include a transaction device identifier and wherein said transaction device random number is provided to said RFID reader in POS pre-defined format, in order to synchronize the system.

15. Claim 15 recites the same limitations as claim 1 and is therefore rejected under the same art and rationale.

Claim Rejections - 35 USC § 102

16. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

17. Claim 16 is rejected under 35 U.S.C. 102(e) as being anticipated by Johnson, Jr. (6,185,307 B1).

Art Unit: 3627

18. Re claim 16, Johnson et al. disclose a method further comprising the steps of generating a reader random number, at the RFID reader, using a reader random number generator (see e.g. col. 3, lines 32-33 – *The POS device will generate authentication check data, preferably a random number*); and validating at least one of the transaction device and the reader in accordance with at least one of the transaction device random number and the reader random number (See e.g. col. 3, lines 41-47, col. 11, lines 22-35).

19. Claim 17 is rejected under 35 U.S.C. 103(a) as being unpatentable over Perron et al. (US 2002/0047049 A1), as supported by the provisional (60/230,914), in view of Atalla (4,268,715), in further view of Mori et al. (6,085,168).

20. Re claim 17, Perron et al. disclose a method for securing a transaction comprising
-generating a transaction device random number at a transaction device, wherein the transaction device includes a random number generator located at the transaction device, wherein the transaction device is associated with a transaction device identifier (Personal identification numbers (PINs)), and a transaction device authentication tag (the random internal number generated by the device), the transaction device identifier being different from the transaction device authentication tag (see e.g. paragraphs 0009, 0029 – *The device randomly generates an internal number using one of more different methods. This random internal number, or at least a portion thereof, can be either divided to form the serial number and the key number; The card 2 can even be designed to generate two or more random internal numbers*);
-transmitting, from the transaction device, the transaction device identifier (card number), the transaction device authentication tag (Personal identification numbers (PINs)), and the transaction device random number (the random internal number generated by the device) to a transaction device reader, wherein the transaction device reader is associated with a reader

Art Unit: 3627

authentication tag (See e.g. paragraphs 0032, 0009; 0033 – 0034 – *the serial number (from the generated random number) or any other identification number and the updated counter valued are obtained from the corresponding memory of card 2, such as the RAM 31 or the EEPROM 32, to form portions of a data stream that is to be transferred to the transaction system*).

-transmitting, from the transaction device reader, the transaction device identifier, the transaction device authentication tag, the transaction device random number, and the transaction device authentication tag to an account issuer associated with the transaction device; validating, at the account issuer, the transaction device based at least in part on both the transaction device identifier and the transaction device authentication tag, both having been received from the transaction device, (See e.g. paragraphs 0033 – 0034 – *the serial number or any other identification number and the updated counter value are obtained from the corresponding memory of card 2, to form portions of a data stream that is to be transferred to the transaction system; Once the data stream is received, the transaction system generally finds the record of the card 2 or that of end user with the serial number or any other number and then determines with the signature if the transaction is legitimate or not*).

Perron et al. do not explicitly disclose a method wherein the transaction device random number is used to decrypt at least one of the transaction device identifier and the transaction device authentication tag, the transaction device random number having been received from the transaction device.

However, Attala discloses a method wherein the transaction device random number is used to decrypt at least one of the transaction device identifier and the transaction device authentication tag, the transaction device random number having been received from the

Art Unit: 3627

transaction device; wherein the transaction device random number is used to decrypt the transaction device reader authentication tag (see e.g. col. 5, lines 47-54).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention to modify Johnson JR., in view of Seidman et al., and include the steps wherein the transaction device random number is used to decrypt at least one of the transaction device identifier, and the transaction device authentication tag, as taught by Atalla, in order to provide secure data transmission, via a multilevel encryption, during the authentication of the transaction.

Perron et al., in view of Atalla, do not explicitly disclose validating, at the account issuer, the transaction device reader based at least in part on the transaction device reader authentication tag, wherein the transaction device random number is used to decrypt the transaction device reader authentication tag.

However, Mori et al. disclose validating, at the account issuer, the transaction device reader based at least in part on the transaction device reader authentication tag, (see e.g. col. 83, lines 7-11 *-Furthermore, according to the present invention, a transmission intermediate decrypts an encrypted electronic message transmitted from the transmitter using a unique decryption key between the intermediate and the transmitter, thereby easily authenticating the transmitter*).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention to modify Perron et al., in view of Atalla., and include the steps wherein the transaction device random number is used to decrypt at least one of the transaction device identifier, and the transaction device authentication tag, as taught by Mori et al., in order to safely trading in goods (see e.g. col. 2, lines 23).

Response to Arguments

21. Applicant's arguments with respect to the previous claims have been considered, but are moot in view of the new grounds of rejection.

Conclusion

22. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Luna Champagne whose telephone number is (571) 272-7177. The examiner can normally be reached on Monday - Friday 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Florian Zeender can be reached on (571) 272-6790. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

Art Unit: 3627

applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Luna Champagne/

Examiner, Art Unit 3627

July 12, 2010

/F. Ryan Zeender/

Supervisory Patent Examiner, Art Unit 3627